IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue- 5 E-ISSN: 2347-2693

Usage of Multiple Clouds to increase Security in Cloud Computing

Ch. Anjani Kumar[1*]and K. Subba Rao[2]

[1*,2] *Department of Information Technology, JNTUK University, Andhra Pradesh, India*

www.ijcseonline.org

Received: 14/04/2014 Revised: 22 /04/2014 Accepted: 17/05/ 2014 Published: 31 /05/2014

Abstract— In today's world Cloud computing has emerged like as a new model of computing. It is a paradigm shift in the computing history. Cloud services are ready to available without capital investment as they are commoditized. Cloud users may get services in pay per use fashion and enjoy so many benefits of cloud computing including less cost and accessibility from anywhere in the world. However, users have security issues as they outsource their secret business data to cloud and treat the cloud as "untrusted". By using a single cloud service provider there might be the risk of service availability, possibility of failure and insider theft of data. By Moving towards multi clouds can address security problems. This paper aims of investigating how multiple-cloud can increase security and have impact on the usage of the cloud computing usage technology. We built a prototype application to simulate the advantages of using multiple-clouds to increase security. The empirical result shows that multiple-clouds can increase security.

Keywords—Cloud computing; Security; Single cloud; Multiple-clouds; Data integrity; Data intrusion; Service availability

I. Introduction

Cloud computing is used by many organizations and the benefits are realized by general public in many ways. Examples for the Cloud service providers are IBM, Microsoft, Amazon, and Oracle are providing various kinds of cloud services. The services may include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). These services can use by cloud users in pay per use fashion without any investment.

According to Subashini and Kavitha[1] argues that cloud computing is used by small and medium sized companies to increase their capacity to serve for their clients better and generate more revenues by decreasing the existing infrastructure costs. However, for growth of cloud computing, the cloud providers are address security issues in cloud storage with high level priority. It has been observed that a single cloud usage having problems in service availability, failure rate, and insider theft. For this reason there was considerable research into the study of multiple-cloud usage for curbing security problems. This paper provides the necessary insights into the usage of multiple-clouds and the possible reduction in security risk of cloud data storage. Cloud users expect security to their confidential information which has been outsourced to client. The data might include sensitive private personal information, some related health records which is critical and to be secured from malicious insider attacks. Session one describes introduction about cloud computing. The remaining of this paper is structured as follows. Session two describes review of literature. Session three describes how to increase security in cloud computing. Session four describes architecture. Session five describes the proposed prototype to simulate the benefits of using multi-clouds. Session six describes experimental results.While session seven concludes the paper.

II. LITERATURE SURVEY

This session describes brief summary review of related work on cloud computing with respect to security. Multi-shares with secret sharing algorithm was proposed in [2] security for cloud and data integrity. By using cryptographic methods [3], the cloud security was explored. The security risks addressed includes availability of service, data intrusion, and data integrity. This solution uses cloud storage and multi-clouds.

In [4] a survey has been conducted to know various security issues and solutions with respect to a single cloud. In [5] RACS and RAID kind of techniques were used for the cloud security using multiple-clouds. In [6] multi-clouds usage for data integrity was explored by using client centric distributed protocols. In [7] the problem, service availability was focused in only single cloud environment. In [8] there was discussion about some cloud security issues. In [9] to protect cloud data in single cloud environment, cryptography is used. In [10] a security mechanism by name "Depot" is used to single cloud environment. A security mechanism by name "Venus" was proposed in [11] which focused on data integrity issue in single cloud environment. Service availability was focused in [1] in single cloud environment.

In [12] a survey is made on cloud security. In [13] cloud data integrity is focused in single cloud environment. In [14] a new security mechanism was proposed by name "HAIL" for improving service availability in multi-cloud environment. In [15] a survey was done on cloud data integrity in multi-cloud environment. Encrypted cloud VPN technique is used in [16] for data integrity in multi-cloud environment. Cloud security was discussed in [17] in single cloud environment.

The TCCP techniques for cloud data integrity issues and service availability were existed in [18] in single cloud environment. In [19] the ensuring cloud data integrity in single cloud environment by using Homomorphic tokens and erasure

Corresponding Author: *Ch. Anjani Kumar, anjan520@gmail.com* codes. PDP schemes were used for protection of the data integrity in clouds. In [20] cloud computing security was explored in single cloud environment.

III. INCREASE SECURITY IN CLOUD COMPUTING

There are two ways to increase security in cloud computing. The first way is we have to identify the risks existed in cloud computing related to security. The following are three important security risks in cloud computing. The primary risk is data integrity, secondary risk is data intrusion and final risk is service availability. Data integrity causes most of the security problems.

This is because the data is very vulnerable to cloud users. The loss of data integrity is having severe impact on them. So Many researches were found this security risk [15], [21], [22] and [23]. Data intrusion is another security risk which is possible when hackers accessing the sensitive information.

To address such a problem considerable research was done [24], [20]. Service availability is another security risk, which is very important from the view of client. Cloud clients expect round the clock availability of cloud services. So many service availability risks were exposed in [25], [15], [20], and [26]. The second way to increase security in cloud computing is when the clouds are increased then the security is also increased, why because actually a single cloud is also having so many distributed systems, if a hacker is entered in to the cloud and changes the data, then automatically the data in the distributed systems is also going to be changed, then that time multiple clouds can increase the security to the data rather than a single cloud.

IV. ARCHITECTURE

In this paper we proposed an architecture for multiple-clouds which is similar to the one presented in [8]. The architecture has provisioned for multiple clouds that work together. It can be called as cloud within clouds or cloud of clouds. The architecture is as shown in below figure.
As can be seen in below figure, it is evident that the architecture has provisioned for multiple clouds. The data outsourced by clients can store in any cloud. It does mean that the multiple clouds working together. This will automatically improve service availability and reduce the risk of losing data and improve the security. With regard to internal theft strict measures are to be used by cloud service providers.
The above figure shows four clouds named as cloud1, cloud2, cloud3, cloud4, which is called as depsky cloud of clouds. Data is stored in the four clouds by client 1, which means that by storing the data in to the multiple obviously the security also increased. Also shows that data is retrieved by the multiple clouds by client 2 called as architecture of depsky.

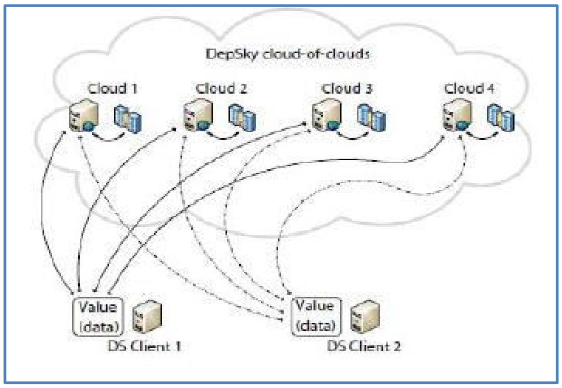


Fig. 1 Architecture of Depsky

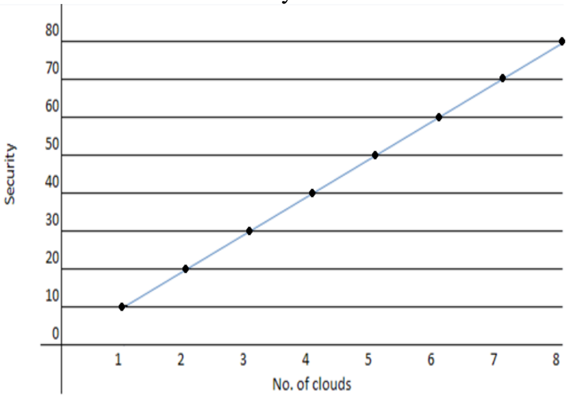
(W/4 clouds, 2 clients)

V. PROTOTYPE APPLICATION

We built a prototype application in the distributed environment. The application demonstrated the presence of multiple clouds and their storage dynamics. This application is built in the Java platform to simulate the multiple-cloud environment. The environment used for the development of an application is a PC with RAM (4 GB), Core 2 dual processor running Windows 7 operating system. Net Beans is the IDE, which is used for the development. The server programs were built in such a way, so that they are working together to reduce the risk of security.

VI. EXPERIMENTAL RESULTS

From the experiments done on the multiple clouds, observed that, when numbers of clouds are increased, then the security is also increased and the risk is reduced. The simulation results reveal this fact. The following is the figure for the number of clouds verses security.



.

Fig. 2 Number of clouds vs. security

As can be seen in above fig. 2, it is evident that the horizontal axis represents number of clouds while the vertical axis represents security. The results reveal that the security is increased when number of clouds is increased.

VII.CONCLUSION

In today's world Cloud computing is rapidly growing. Cloud users are eligible to get services with less cost and greater accessibility. However, their security concerns are addressed. In this paper, we proposed an architecture that makes usage of multiple clouds together to improve service availability and reducing the risk of data losing. We have implemented a custom Java simulator application that demonstrated the usefulness of multiple clouds. The experimental results reveal that the multiple clouds are having capacity of increasing security.

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), **2011**, pp.**1-11**.

[2] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensu [2] M.A. AlZain and E. Pardede, "Using Multi Shares for ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), **2011**, pp.**1-9**.

[3] Bessani, M. Correia, B. Quaresma, F.André and P. Sousa, "DepSky: dependable and EuroSys'11 : Proc. 6th Conf. On Computer Systems, **2011**, pp.**31-46**.

[4] F. Rocha and M. Correia, "Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", Proc. 1st Intl. Workshop of Dependability of Clouds, Data Centers and Virtual Computing Environments, **2011**, pp.**1-6**.

[5] H.Abu-Libdeh, L. Prince house and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10 : Proc 1st ACM symposium on Cloud computing, **2010** , pp.**229-240**.

[6] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Inter cloud", Research Report RZ,3783, **2010**.

[7] A.J. Feldman, W.P. Zeller, M.J. Freedman and E.W. Felten, "SPORC: Group collaboration using untrusted cloud resources", OSDI, October **2010**, pp.**1-14**.

[8] E. Grosse, J. Howie, J. Ransome, J. Reavis and S.Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), **2010**, pp.**17-23**.

[9] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14th Intl.Conf. On Financial cryptograpy and data security, **2010**, pp.**136-149**.

[10] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi,M. Dahlin and M. Walfish, "Depot: Cloud storage with minimal trust", OSDI'10: Proc. of the 9th USENIX Conf. on Operating systems design and implementation, **2010**, pp.**1-16**.

[11] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y.Michalevsky and D. Shaket, "Venus: Verification for untrusted cloud storage", CCSW'10: Proc.ACM workshop on Cloud computing security workshop, **2010**, pp.**19-30**.

[12] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), **2010**, pp. **24-31**.

[13] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing", HotSec'10: Proc. 5th USENIX Conf. on Hot topics in security, **2010**, pp.**1-8**.

[14] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, **2009**, pp.**187-198**.

[15] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, **2009**, pp.**81-86**.

[16] Clavister, "Security in the cloud", Clavister White Paper, **2008**.

[17] T.Ristenpart, E.Tromer, H.Shacham and S.Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds:, CCS'- 09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp.**199-212**.

[18] N. Santos, K.P. Gummadi and R.Rodrigues, "Towards trusted cloud computing", USENIX Association, 2009, pp.**3-3**.

[19] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, **2010**, pp.**1-9**.

[20] S.L. Garfinkel, "An evaluation of Amazon's grid computing services: EC2, S3, and QS", Technical Report TR-08- 07, Computer Science Group, Harvard University, Cite seer, **2007**, pp.**1-15**.

[21] J. Hendricks, G.R. Ganger and M.K. Reiter, "Low over head by zantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, **2007**, pp.**73-86**.

[22] RedHat,https://rhn.redhat.com/errata/RHSA-2008-0855.html.

[23] Sun,http://blogs.sun.com/gbrunett/entry/amazon_s3_silent_data_corruption.

[24] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), **2003**, pp.**20-26**.

[25] Amazon, Amazon Web Services. Web services licensing agreement, October3, **2006**.

[26] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-hashing for message authentication", Cite seer, **1997**, pp.**1-11**.

AUTHORS PROFILE

Chejarla Anjani Kumar pursuing M.Tech Degree in Software Engineering from Lakireddy Balireddy College of Engineering, Vijayawada, AP, INDIA. His main research interest in software engineering,Cloud Computing.

Katta Subba Rao is presently Associate Professor in Dept. of Information Technology, Lakireddy Balireddy College of Engineering, Vijayawada. He is currently submitted the PhD thesis in Software Engineering area from ANU.